FORTRA™

DATASHEET (PHISHLABS)

Proactively Monitor for Stolen and Leaked Credentials

Use of stolen credentials leads the way in tactics used by threat actors according to Verizon's 2023 Data Breach Investigation Report. Compromised credentials can wreak havoc on an organization through data breaches, reputational damage, and account takeovers. Monitoring for these threats are essential but come with multiple burdens. Lack of broad visibility, access, and knowledge can keep threat actors steps ahead of organizations.

Fortra's PhishLabs provides the ability to quickly respond and implement countermeasures to guard against attacks. PhishLabs' Compromised Credentials Monitoring delivers broad visibility into stolen employee and customer credentials revealed from dark web sites and harvested from third-party leaks, infostealers, botnets, and other forms of malware. The enhanced visibility allows organizations to quickly respond and implement countermeasures, such as forced password resets and lockouts to guard against potential account takeovers, breaches, and malware attacks.

Compromised Credentials Monitoring Capabilities

Expose Threats Quickly

Enhance the detection of compromised credentials on dark web forums, websites, and blogs, as well as compromises caused by third-party leaks, botnets, infostealers and other malware.

Expert Curation

PhishLabs' team of dark web analysts refine incident search results provided by external feeds and internal proprietary technology to quickly separate relevant threats from the noise.

Protect Employees and Customers

Detect both employee and customer compromised credentials for sale, whether leaked internally or stolen by threat actors.

PRODUCT SUMMARY

PhishLabs' Compromised Credentials Monitoring provides broad visibility into actionable employee and customer stolen credentials uncovered from dark web sites and harvested through malware, to proactively guard against future attacks.

KEY FEATURES

Organizations can expose threats quickly through enhanced detection of compromised credentials caused by the following:

- Third-party leaks
- Infostealers
- Botnets
- And other malware

The enhanced visibility provides organizations the ability to quickly respond and implement countermeasures, such as:

- Forced password resets
- Account lockouts
- Stop the exfiltration of outbound transfers in-flight

Exclusive Insights

Gain access to rich credential data that is fully actionable and not protected behind paywalls.

Proactively Defend

Guard against potential attacks by implementing countermeasures designed to protect your organization's brand, employees, and customers through forced password resets, account lockouts, and by stopping the exfiltration of outbound transfers in-flight.

Comprehensive Protection Against Dark Web Threats

Uncover brand threats and compromised credentials across anonymized dark web sites and malware with PhishLab's Dark Web Monitoring.

Dark Web Brand Monitoring
Dark sites, marketplaces and forums

Brand and Executive mentions, Stolen PII, card data, BINs, emails Phishing kits, Fraud tools Initial Access Brokers

Continuous targeted surveillance
Monitor for changes in activity

Compromised Credentials Monitoring
Infostealers, botnets and other malware

Actionable compromised logins
Emails, passwords, secret codes
Not parked behind paywalls

Implement proactive countermeasures
Forced password resets/account lockouts
Stop exfiltration of outbound transfers

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.